The Gaussian Wiretap Channel with a Helping Interferer

Xiaojun Tang*, Ruoheng Liu†, Predrag Spasojević*, and H. Vincent Poor†
*Rutgers University, {xtang,spasojev}@winlab.rutgers.edu
†Princeton University, {rliu,poor}@princeton.edu

***Abstract*— Due to the broadcast nature of the wireless medium, wireless communication is susceptible to adversarial eavesdropping. This paper describes how eavesdropping can potentially be defeated by exploiting the superposition nature of the wireless medium. A Gaussian wire-tap channel with a helping interferer (WTC-HI) is considered in which a transmitter sends confidential messages to its intended receiver in the presence of a passive eavesdropper and with the help of an interferer. The interferer, which does not know the confidential message assists the confidential message transmission by sending a signal that is independent of the transmitted message. An achievable secrecy rate and a Sato-type upper bound on the secrecy capacity are given for the Gaussian WTC-HI. Through numerical analysis, it is found that the upper bound is close to the achievable secrecy rate when the interference is weak for symmetric interference channels, and under more general conditions for asymmetric Gaussian interference channels.**

I. Introduction

Broadcast and superposition are two fundamental properties of the wireless medium. Due to the broadcast nature, wireless transmission can be heard by multiple receivers with possibly different signal strengths. Due to the superposition nature, a receiver observes a signal that is a superposition of multiple simultaneous transmissions. From the *secure communication* point of view, the two properties are interwoven and pose a number of security issues. In particular, the broadcast nature makes wireless transmission susceptible to *eavesdropping* since anyone within the communication range can listen and possibly extract information. A helper can pit one property of the wireless medium against security issues caused by the other. In this paper, we consider the case in which a helper functions as an interferer to improve the secrecy level of a communication session that is compromised by a passive eavesdropper. This phenomenon illustrates that superposition can *enhance* security.

As depicted in Fig. 1, we study the problem in which a transmitter sends confidential messages to an intended receiver with the help of an interferer, in the presence of a passive eavesdropper. We call this model the *wiretap channel with a helping interferer* (WTC-HI). Here, it is desirable to minimize the leakage of information to the eavesdropper. The secrecy level, i.e., the level of ignorance of the eavesdropper with respect to the confidential message, is measured by the equivocation rate. This information-theoretic approach was introduced by Wyner [1] for the *wiretap channel* problem,

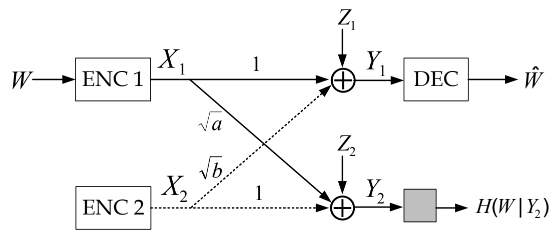

Fig. 1. A Gaussian wiretap channel with a helping interferer.

in which a single source-destination communication is eavesdropped upon via a degraded channel. Wyner's formulation was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2]. The Gaussian wiretap channel was considered in [3]. The central idea is that the transmitter uses stochastic encoding [2] to introduce *randomness*, and hence increase secrecy. In the WTC-HI model, the helper provides additional randomization via stochastic encoding without knowing the transmitted message.

In this paper, we give an achievable secrecy rate for the Gaussian WTC-HI under the requirement that the eavesdropper is kept in total ignorance with respect to the message for the intended receiver. The results show that the interferer can indeed increase the secrecy level, and that a positive secrecy rate can be achieved even when the source-destination channel is worse than the source-eavesdropper channel. We also describe a power control strategy for maximizing the achievable secrecy rate. In addition, we provide a Sato-type upper bound on the secrecy capacity of the Gaussian WTC-HI. Through numerical analysis, we find that the upper bound is close to the achievable secrecy rate when the interference is weak for symmetric interference channels, and under more general conditions for asymmetric Gaussian WTC-HIs.

Related work includes the multiple access channel with confidential messages [4]–[7], the interference channel with confidential messages [8], [9], and the relay channel with confidential messages [10]–[12]. Our achievable scheme can be considered to be a generalization of the two schemes of [6] and [11]. The cooperative jamming scheme of [6] considers the situation in which encoder 2 generates independent Gaussian noise. This scheme does not employ any structure in the transmitted signal. The noise forwarding scheme of [11] requires that the interferer's codewords can always be decoded by the intended receiver which is not necessary in our scheme. In addition, no work describes a computable upper bound on the secrecy capacity of the Gaussian WTC-HI.

This research was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208.

The remainder of the paper is organized as follows. Section II describes the system model and problem formulation. Section III states our achievability results. Section IV gives the upper bound. Section V illustrate the results through some numerical examples. The paper is concluded in Section VI.

II. System Model

The system consists of a transmitter, an intended receiver, a helping interferer, and a passive eavesdropper. The transmitter sends a confidential message W to the intended receiver with the help from an *independent* interferer, in the presence of passive but *intelligent* eavesdropper (who knows both codebooks). As illustrated in Fig. 1, the channel outputs at the intended receiver and the eavesdropper can be written as

$$Y_{1,k} = X_{1,k} + \sqrt{b}X_{2,k} + Z_{1,k}, \tag{1a}$$

$$Y_{2,k} = \sqrt{a}X_{1,k} + X_{2,k} + Z_{2,k}, \tag{1b}$$

for $k = 1, \ldots, n$, where $\{Z_{1,k}\}$ and $\{Z_{2,k}\}$ are sequences of independent and identically distributed zero-mean Gaussian noise variables with unit variances. The channel inputs $X_{1,k}$ and $X_{2,k}$ satisfy average block power constraints of the form

$$\frac{1}{n}\sum_{k=1}^{n} E[X_{1,k}^2] \le \bar{P}_1 \quad \text{and} \quad \frac{1}{n}\sum_{k=1}^{n} E[X_{2,k}^2] \le \bar{P}_2. \tag{2}$$

The transmitter uses encoder 1 to encode confidential message $w \in \mathcal{W} = \{1, \ldots, M\}$ into x^n and sends it to the intended receiver in n channel uses. A stochastic encoder f_1 is specified by a matrix of conditional probabilities $f_1(x_{1,k}|w)$, where $x_{1,k} \in \mathcal{X}$, $w \in \mathcal{W}$, $\sum_{x_{1,k}} f_1(x_{1,k}|w) = 1$ for all $k = 1, \ldots, n$, and $f_1(x_{1,k}|w)$ is the probability that encoder 1 outputs $x_{1,k}$ when message w is being sent. The helper generates its output $x_{2,k}$ randomly and can be considered as using another stochastic encoder f_2, which is specified by a matrix of conditional probabilities $f_2(x_{2,k})$ with $x_{2,k} \in \mathcal{X}_2$ and $\sum_{x_{2,k}} f_2(x_{2,k}) = 1$. Hence, encoder 1 uses stochastic encoding to introduce *randomness* and increase secrecy. Additional randomization is provided by the helper and the secrecy is further increased.

The decoder uses the output sequence y_1^n to compute its estimate $\hat{w}$ of w. The decoding function is specified by a (deterministic) mapping $\phi : \mathcal{Y}_1^n \rightarrow \mathcal{W}$.

An (M, n, P_e) code for the Gaussian WTC-HI consists of two sets of n encoding functions $f_{1,k}$ and $f_{2,k}$, $k = 1, \ldots, n$ and a decoding function ϕ so that its average probability of error is

$$P_e = \frac{1}{M}\sum_{w} \Pr\left\{\phi(Y_1^n) \neq w | w \text{ sent}\right\}. \tag{3}$$

The secrecy level (level of ignorance of the eavesdropper with respect to the confidential message w) is measured by the equivocation rate[1] $\frac{1}{n}H(W|Y_2^n)$.

A secrecy rate R_s is achievable for the Gaussian WTC-HI if, for any $\epsilon > 0$, there exists an (M, n, P_e) code so that

$$M \ge 2^{nR_s}, \; P_e \le \epsilon \tag{4}$$

$$\text{and} \qquad R_s - \frac{1}{n}H(W|Y_2^n) \le \epsilon \tag{5}$$

for all sufficiently large n. The secrecy capacity is the maximal achievable secrecy rate.

III. Achievable Secrecy Rate

In this section, we consider an achievable secrecy rate by assuming that the transmitter and the interferer transmit with powers $P_1 \le \bar{P}_1$ and $P_2 \le \bar{P}_2$, respectively. We address the power control issue in Subsection III-B.

A. Achievable Secrecy Rate

Theorem 1: The following secrecy rate is achievable for the Gaussian WTC-HI:

$$R_s(P_1, P_2) = \begin{cases} 0 & \text{if } a \ge 1 + P_2, \\ R_s^{\mathrm{I}}(P_1, P_2) & \text{if } 1 \le a < 1 + P_2, \\ R_s^{\mathrm{II}}(P_1, P_2) & \text{if } a < 1, \end{cases} \tag{6}$$

where $R_s^{\mathrm{I}}(P_1, P_2)$ and $R_s^{\mathrm{II}}(P_1, P_2)$ are given by

$$R_s^{\mathrm{I}}(P_1, P_2) = \begin{cases} \mathsf{g}(P_1) - \mathsf{g}(\frac{aP_1}{1+P_2}) & \text{if } b \ge 1 + P_1, \\ \left[\mathsf{g}(P_1 + bP_2) - \mathsf{g}(aP_1 + P_2)\right]^+ & \text{if } 1 \le b < 1 + P_1, \\ \left[\mathsf{g}(\frac{P_1}{1+bP_2}) - \mathsf{g}(\frac{aP_1}{1+P_2})\right]^+ & \text{if } b < 1, \end{cases}$$

and

$$R_s^{\mathrm{II}}(P_1, P_2) = \begin{cases} \mathsf{g}(P_1) - \mathsf{g}(\frac{aP_1}{1+P_2}) & \text{if } b \ge 1 + P_1, \\ \mathsf{g}(P_1 + bP_2) - \mathsf{g}(aP_1 + P_2) & \text{if } \beta_1 \le b < 1 + P_1, \\ \mathsf{g}(P_1) - \mathsf{g}(aP_1) & \text{if } \beta_2 \le b < \beta_1, \\ \mathsf{g}(\frac{P_1}{1+bP_2}) - \mathsf{g}(\frac{aP_1}{1+P_2}) & \text{if } b < \beta_2, \end{cases}$$

with $\mathsf{g}(x) \triangleq (1/2)\log_2(1 + x)$,

$$\beta_1 = \frac{1 + P_1}{1 + aP_1} \quad \text{and} \quad \beta_2 = \frac{a(1 + P_1)}{1 + aP_1 + (1 - a)P_2}.$$

Proof: We briefly outline the achievability scheme next and omit the details of the proof.

In the scheme, we use two independent Gaussian codebooks. Encoder 1 uses stochastic codebook $\mathcal{C}_1(2^{nR_1}, 2^{nR_s}, n)$, where 2^{nR_1} is the size of the codebook, and 2^{nR_s} is the number of confidential messages can be conveyed ($R_s \le R$). The 2^{nR_1} codewords in codebook $\mathcal{C}_1$ are randomly grouped into 2^{nR_s} bins each with $M = 2^{n(R_1 - R_s)}$ codewords. In addition, encoder 2 uses codebook $\mathcal{C}_2(2^{nR_2}, 1, n)$, where 2^{nR_2} is the codebook size and the whole codebook forms a single bin. To send message $w \in [1, \ldots, 2^{nR_s}]$, encoder 1 randomly selects a codeword from the w-th bin to send, and encoder 2 randomly selects a codeword from codebook $\mathcal{C}_2$ to send.

The achievable rate given in Theorem 1 is derived by using the above coding scheme and properly choosing the coding parameter triple (R_1, R_s, R_2). ■

[1]The secrecy defined by equivocation rate is weak and can be strengthened using extractor functions without loss of secrecy rate as shown in [13].

Remark 1: It is clear that an interference power P_2 can benefit secrecy. In particular, when P_2 is sufficiently large, a positive secrecy rate can be achieved except the case

$$a^{-1} \leq b < 1.$$

For comparison, we recall that the secrecy capacity of the Gaussian wiretap channel (when there is no interferer in the Gaussian WTC-HI model) is

$$R_s^{\mathrm{WT}} = [\mathrm{g}(P_1) - \mathrm{g}(aP_1)]^+ \tag{7}$$

and positive secrecy rate can be achieved only when $a < 1$.

B. Power Control

Power control is essential to interference management when accommodating multi-user communications. As for the Gaussian WTC-HI, power control also plays a critical role. The interferer may need to control its power so that it does not introduce too much interference to the primary transmission, while the transmitter may want to select its power so that the intended receiver is able to decode and cancel some now helpful interference before decoding the primary transmission.

In this section, we consider a power control strategy for maximizing the secrecy rate given in Theorem 1. We consider the cases with $a \geq 1$ and $a < 1$, respectively. Due to space limitations, we omit the proof.

1) $a \geq 1$:

Proposition 1: When $a \geq 1$, the power control scheme for maximizing the secrecy rate is given by

$$(P_1, P_2) = \begin{cases} (\min\{\bar{P}_1, P_1^*\}, \bar{P}_2) & \text{if } b > 1, \bar{P}_2 > a - 1, \\ (\bar{P}_1, \min\{\bar{P}_2, P_2^*\}) & \text{if } b < \frac{1}{a}, \bar{P}_2 > \frac{a-1}{1-ab}, \\ (0, 0) & \text{otherwise,} \end{cases}$$

where $P_1^* = b - 1$ and

$$P_2^* = \frac{a - 1 + \sqrt{(a-1)^2 + (b^{-1} - a)[a - b + (1-b)a\bar{P}_1]}}{1 - ab}. \tag{8}$$

According to Proposition 1, when $a > 1$, a positive secrecy rate can be achieved when $b > 1$ or $b \leq a^{-1}$ if the interferer's power $\bar{P}_2$ is large enough. When $b > 1$, the interferer uses its full power $\bar{P}_2$ and the transmitter selects its power to guarantee that the intended receiver can first decode the interference (and cancel it). When $b < a^{-1}$, the intended receiver treats the interference as noise. In this case, the transmitter can use its full power $\bar{P}_1$ and the interferer controls its power (below P_2^*) to avoid excessive interference.

2) $a < 1$:

Proposition 2: When $a < 1$, the power control scheme for maximizing the secrecy rate is given by

$$(P_1, P_2) = \begin{cases} (\bar{P}_1, \bar{P}_2) & \text{if } b \geq 1, \bar{P}_1 < b - 1, \\ (\bar{P}_1, \bar{P}_2) & \text{if } b \geq \frac{1}{a}, \bar{P}_1 \geq b - 1, \bar{P}_2 < \frac{1-a}{ab-1}, \\ (P_1^*, \bar{P}_2) & \text{if } b \geq \frac{1}{a}, \bar{P}_1 \geq b - 1, \bar{P}_2 \geq \frac{1-a}{ab-1}, \\ (\bar{P}_1, \bar{P}_2) & \text{if } 1 \leq b < \frac{1}{a}, b - 1 \leq \bar{P}_1 < \frac{b-1}{1-ab}, \\ (\bar{P}_1, \min\{\bar{P}_2, P_2^*\}) & \text{if } b < 1, \bar{P}_1 \geq \frac{b-a}{a(1-b)}, \\ (\bar{P}_1, 0) & \text{otherwise,} \end{cases}$$

where $P_1^* = b - 1$ and P_2^* is given by (8).

When $a < 1$, positive secrecy rate is always feasible. Here, we consider the cases when the interferer does not help. First, in the case when $1 \leq b < a^{-1}$, the transmitter needs to hold its power if it wants to let the receiver decode some interference. However, if the transmitter has a large power ($\bar{P}_1 > \frac{b-1}{1-ab}$), it would better to use all its power and request the interferer be silent. In the case when $a < b < 1$, the receiver treats the interference as noise. If the transmitter does not have enough power ($\bar{P}_1 < \frac{b-a}{a(1-b)}$), the interference will hurt the intended receiver more than the eavesdropper.

C. Power-unconstrained Secrecy Rate

A fundamental parameter of wiretap-channel-based wireless secrecy systems is the secrecy rate when the transmitter has unconstrained power, which is only related to the channel conditions. For example, the power-unconstrained secrecy capacity for the Gaussian wiretap channel is given by

$$\lim_{\bar{P}_1 \to \infty} \left[\mathrm{g}(\bar{P}_1) - \mathrm{g}(a\bar{P}_1)\right]^+ = \frac{1}{2}\left[\log_2 \frac{1}{a}\right]^+. \tag{9}$$

After some limiting analysis, we have the following result for the Gaussian WTC-HI model.

Theorem 2: When $a \geq 1$, the achievable power unconstrained secrecy rate for the Gaussian WTC-HI is

$$\lim_{\bar{P}_1, \bar{P}_2 \to \infty} R_s = \begin{cases} \frac{1}{2}\log_2 b & \text{if } b > 1, \\ \frac{1}{2}\log_2 \frac{1}{ab} & \text{if } b < \frac{1}{a}, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

When $a < 1$, the achievable power unconstrained secrecy rate for the Gaussian WTC-HI is

$$\lim_{\bar{P}_1, \bar{P}_2 \to \infty} R_s = \begin{cases} \frac{1}{2}\log_2 b & \text{if } b > \frac{1}{a}, \\ \frac{1}{2}\log_2 \frac{1}{ab} & \text{if } b < 1, \\ \frac{1}{2}\log_2 \frac{1}{a} & \text{otherwise.} \end{cases} \tag{11}$$

When the interference is weak ($b < a^{-1}$ if $a \geq 1$, or $b < 1$ if $a < 1$), the interference introduces a gain of $(1/2)\log_2(1/b)$. When the interference is strong enough ($b > 1$ if $a \geq 1$, or $b > a^{-1}$ if $a < 1$), the power-unconstrained secrecy rate is $(1/2)\log_2 b$. Note that $(1/2)\log_2 b$ is the power-unconstrained secrecy rate if the confidential message is sent from the interferer to the intended receiver in the presence of the eavesdropper. This is particularly interesting because we do not assume that there is a transmitter-interferer channel (which would enable the interferer to relay the transmission).

IV. Sato-Type Upper Bound

In this section, we first describe a computable Sato-type upper bound for a general WTC-HI and next evaluate the upper bound for the Gaussian WTC-HI.

It should be noted that the secrecy capacity of the WTC-HI depends only on the marginal distributions $P_{Y_1|X_1,X_2}$ and $P_{Y_2|X_1,X_2}$, and not on any further structure of the joint distribution $P_{Y_1,Y_2|X_1,X_2}$. In fact, the secrecy capacity is the same for any channel described by $P_{\tilde{Y}_1,\tilde{Y}_2|X_1,X_2}$ whose marginal distributions satisfy

$$P_{\tilde{Y}_j|X_1,X_2}(y_j|x_1,x_2) = P_{Y_j|X_1,X_2}(y_j|x_1,x_2) \tag{12}$$

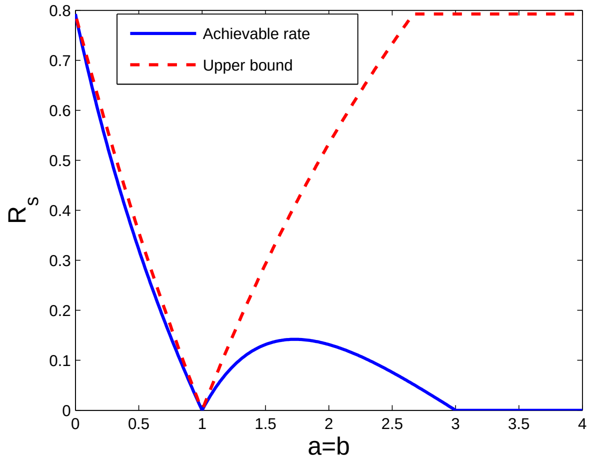

Fig. 2. Achievable secrecy rate and upper bound versus channel gain $a = b$ for a symmetric channel.

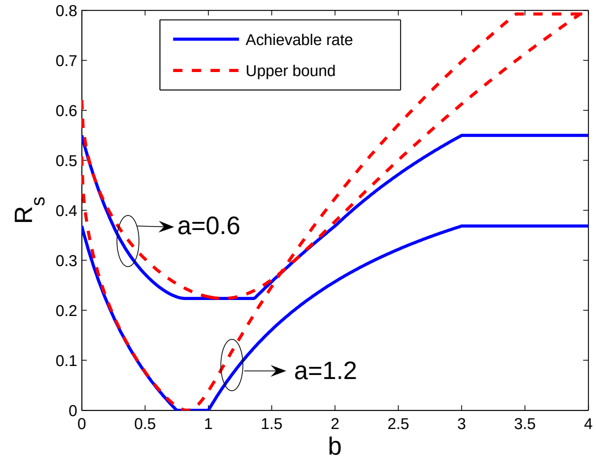

Fig. 3. Achievable secrecy rate and upper bound versus b.

for $j = 1, 2$ and all y_1, y_2 and x_1, x_2.

Theorem 3: Let R_u denote a Sato-type upper bound

$$R_u \triangleq \min_{P_{\tilde{Y}_1,\tilde{Y}_2|X_1,X_2}} \max_{P_{X_1},P_{X_2}} I(X_1, X_2; \tilde{Y}_1|\tilde{Y}_2). \tag{13}$$

Then, the secrecy capacity of WTC-HI satisfies

$$R_s \leq \min \left[R_u, \max_{P_{X_1},P_{X_2}} I(X_1; Y_1|X_2) \right]. \tag{14}$$

Proof: The proof can be found in the Appendix. ■

The upper bound assumes that a genie gives the eavesdropper's signal $\tilde{Y}_2$ to the intended receiver as the side information for decoding message W. Since the eavesdropper's signal $\tilde{Y}_2$ is always a degraded version of the combined signal $(\tilde{Y}_1, \tilde{Y}_2)$, the wiretap channel result [1] can therefore be used.

Now we consider the evaluate of (13) for the Gaussian WTC-HI. $I(X_1, X_2; \tilde{Y}_1|\tilde{Y}_2)$ is a function of the transmit power P_1, P_2 and the noise covariance ρ. Hence, it is denoted as $f(P_1, P_2, \rho)$ and is shown to be

$$f(P_1, P_2, \rho) = \frac{1}{2}\times$$
$$\log_2 \frac{(1 + P_1 + bP_2)(1 + aP_1 + P_2) - (\rho + \sqrt{a}P_1 + \sqrt{b}P_2)^2}{(1 - \rho^2)(1 + aP_1 + P_2)}. \tag{15}$$

For any given ρ, $f(P_1, P_2, \rho)$ is an increasing function of both P_1 and P_2. For any given P_1 and P_2, $f(P_1, P_2, \rho)$ is a convex function of ρ and the minimum occurs when ρ is chosen to be $\rho^\star$, which is given by

$$\rho^\star(P_1, P_2) = \frac{(1 + a)P_1 + (1 + b)P_2 + (\sqrt{ab} - 1)^2 P_1 P_2 - \sqrt{\Delta}}{2(\sqrt{a}P_1 + \sqrt{b}P_2)}$$

where

$$\Delta = [(\sqrt{a} - 1)^2 P_1 + (\sqrt{b} - 1)^2 P_2 + (\sqrt{ab} - 1)^2 P_1 P_2] \times [(\sqrt{a} + 1)^2 P_1 + (\sqrt{b} + 1)^2 P_2 + (\sqrt{ab} - 1)^2 P_1 P_2].$$

Therefore, the Sato-type upper bound can be calculated as

$$R_u = \min_{\rho} \max_{(P_1,P_2)} f(P_1, P_2, \rho) = f(\bar{P}_1, \bar{P}_2, \rho^*(\bar{P}_1, \bar{P}_2)).$$

V. Numerical Examples

Fig. 2 shows the achievable rate and the modified Sato-type upper bound for a symmetric Gaussian WTC-HI channel ($a = b$). In this example, we assume that $\bar{P}_1 = \bar{P}_2 = 2$, and a varies from 0 to 4. The achievable rate R_s first decreases with a when $a < 1$; when $1 < a \leq 1.73$, R_s increases with a because the intended receiver now can decode and cancel the interference, while the eavesdropper can only treat the interference as noise; when $a > 1.73$, R_s decreases again with a because the interference does not affect the eavesdropper much when a is large. The upper bound is good for the weak interference case when $a \leq 1$. However, when $a > 1$ and a is large, the upper bound is quite loose because too much information is given to the intended receiver in the genie-aided bound.

In Fig. 3 and Fig. 4, we present numerical results to show the achievable rate and the modified Sato-type upper bound for the general parameter settings of a and b, where we again assume that $\bar{P}_1 = \bar{P}_2 = 2$. In Fig. 3, we show the secrecy rate versus b when a is fixed to be 0.6 and 1.2, respectively. In Fig. 4, we show the secrecy rate versus a when b is fixed to be 0.2 and 1.2, respectively. Our numerical results show that the Sato-type upper bound is good when $ab \leq 1$ (which is consistent with $a \leq 1$ for the symmetric case). Note that $ab = 1$ corresponds to the degraded case, for which the Sato-type upper bound is always tight.

VI. Conclusions

In this paper, we have considered the use of the superposition property of the wireless medium to alleviate the eavesdropping issues caused by the broadcast nature of the medium. We have studied a Gaussian wiretap channel with a helping interferer, in which the interferer assists the secret communication by injecting independent interference. We have given an achievable secrecy rate and a Sato-type upper bound on the secrecy capacity. The results show that interference, which seldom offers any advantage for (Gaussian) problems

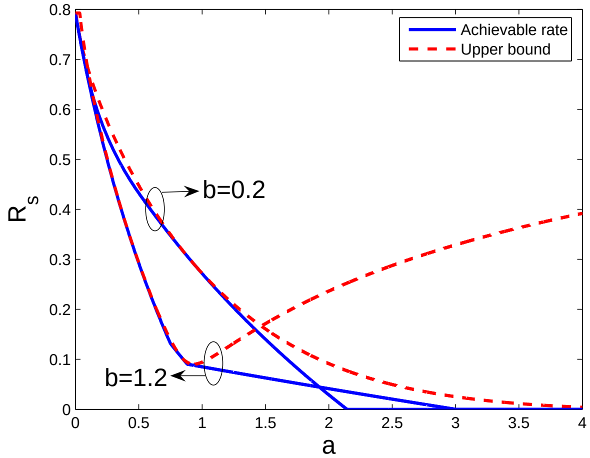

Fig. 4. Achievable secrecy rate and upper bound versus a.

not involving secrecy, can benefit secret wireless communication.

APPENDIX

Proof: [Proof of Theorem 3]

The secrecy requirement implies that

$$nR_s = H(W) \le H(W|Y_2^n) + n\epsilon, \tag{16}$$

and Fano's inequality implies that

$$H(W|Y_1^n) \le n\epsilon R_1 + h(\epsilon) \triangleq n\delta. \tag{17}$$

Based on (16) and (17), we have

$$\begin{aligned} nR_s &\le H(W|Y_2^n) + n\epsilon \\ &\le H(W|Y_2^n) - H(W|Y_1^n) + n(\epsilon+\delta) \\ &\le H(W|Y_2^n) - H(W|Y_1^n, Y_2^n) + n(\epsilon+\delta) &(18)\\ &= I(W; Y_1^n|Y_2^n) + n(\epsilon+\delta) \\ &\le I(X_1^n, X_2^n; Y_1^n|Y_2^n) + n(\epsilon+\delta) &(19)\\ &\le \sum_{i=1}^{n} I(X_{1,i}, X_{2,i}; Y_{1,i}|Y_{2,i}) + n(\epsilon+\delta), &(20) \end{aligned}$$

where (18) is due to the fact that conditioning reduces entropy, and (19) follows since $W \to (X_1^n, X_2^n) \to (Y_1^n, Y_2^n)$ forms a Markov chain. Since the secrecy capacity of the WTC-HI depends only on marginal distributions, we can replace (Y_1, Y_2) with $(\tilde{Y}_1, \tilde{Y}_2)$ defined by (12) and obtain (13).

Now we evaluate (13) for the Gaussian WTC-HI. We let

$$\tilde{Y}_1 = X_1 + \sqrt{b}X_2 + \tilde{Z}_1 \text{ and } \tilde{Y}_2 = \sqrt{a}X_1 + X_2 + \tilde{Z}_2, \tag{21}$$

where $\tilde{Z}_1$ and $\tilde{Z}_2$ are arbitrarily correlated Gaussian random variables with zero-means and unit variances. Let ρ denote the covariance between $\tilde{Z}_1$ and $\tilde{Z}_2$, i.e.,

$$\mathrm{Cov}(\tilde{Z}_1, \tilde{Z}_2) = \rho.$$

Now, $I(X_1, X_2; \tilde{Y}_1|\tilde{Y}_2)$ can be evaluated as

$$\begin{aligned} &I(X_1, X_2; \tilde{Y}_1|\tilde{Y}_2) \\ &= I(X_1, X_2; \tilde{Y}_1, \tilde{Y}_2) - I(X_1, X_2; \tilde{Y}_2) \\ &= [H(\tilde{Y}_1, \tilde{Y}_2) - H(\tilde{Y}_1, \tilde{Y}_2|X_1, X_2)] - [h(\tilde{Y}_2) - h(\tilde{Y}_2|X_1, X_2)] \\ &= h(\tilde{Y}_1|\tilde{Y}_2) - h(\tilde{Z}_1|\tilde{Z}_2) \\ &= h(\tilde{Y}_1|\tilde{Y}_2) - \frac{1}{2}\log_2[2\pi e(1-\rho^2)]. &(22) \end{aligned}$$

By letting

$$t = \frac{E[\tilde{Y}_1\tilde{Y}_2]}{E[\tilde{Y}_2^2]}, \tag{23}$$

we have

$$\begin{aligned} h(\tilde{Y}_1|\tilde{Y}_2) &= h(\tilde{Y}_1 - t\tilde{Y}_2|\tilde{Y}_2) \\ &\le h(\tilde{Y}_1 - t\tilde{Y}_2) &(24)\\ &\le \frac{1}{2}\log_2[2\pi e \mathrm{Var}(\tilde{Y}_1 - t\tilde{Y}_2)], &(25) \end{aligned}$$

where (25) follows from the maximum-entropy theorem and both equalities in (24) and (25) hold true when (X_1, X_2) are Gaussian.

Furthermore, we have

$$\mathrm{Var}(\tilde{Y}_1 - t\tilde{Y}_2) = 1 + P_1 + bP_2 - \frac{(\rho + \sqrt{a}P_1 + \sqrt{b}P_2)^2}{1 + aP_1 + P_2}.$$

Hence, $I(X_1, X_2; \tilde{Y}_1|\tilde{Y}_2)$ can be evaluated by (15). ■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[5] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, USA, July 2006.

[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008, to appear.

[7] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Lake Tahoe, CA, USA, Sept. 2007.

[8] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008, to appear.

[9] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Cognitive interference channels with confidential messages," in *Proc. 45th Annual Allerton Conference on Commun. Contr. Computing*, Monticello, IL, USA, Sept. 2007.

[10] Y. Oohama, "Coding for relay channels with confidential messages," in *IEEE Inf. Theory Workshop*, Cairns, Australia, Sept. 2001, pp. 87–89.

[11] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, Dec. 2006, submitted.

[12] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, Mar. 2007.

[13] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *EUROCRYPT, Lecture Notes in Computer Science*, vol. 1807. Springer-Verlag, 2000, pp. 351–368.